Lab 6: Online and offline password guessing

- cilj ovih vježbi bio je simulirati online i offline napade.
- kod online napada napadač komunicira sa serverom
- kod offline napada napadač nije na mreži sa serverom

1. **online napad**

- trebamo se spojiti na lokalno računalo pomocu ssh ali nam je potrebna lozinka koju moramo saznati
- lozinka ima 4-6 slova i sva su mala
  - broj kombinacija lozinki: 26^4 + 26^5 + 26^6 ≈ 320 000 000
- brute force napadom brzina je 64 hash/min pa bi nam trebalo otprilike 8 godina da pogodimo lozinku
- zatim smo koristili već kreirani dictionary u kojem su se nalazile neke odabrani pokušaji za pogađanje lozinke te je ovaj napad puno brži od prethodnog jer ima puno manje mogućnosti za lozinku

2. **offline napad**

- uspoređujemo hash vrijednosti lozinki koje pokušavamo s onim hash vrijednostima koje su zapisane u bazi
- one su nam poznate jer imamo popis korisnika s njihovim hashevima
- odabrali smo nekog korisnika i njegov hash spremili u dokument
- i u offline napadu napad je pomoću pripremljenog dictionarya brži